final part of the data block is an encryption checksum 158, which is added by the encryption function and checked and removed by the decryption function to ensure that the data block has been received correctly after transmission.--

IN THE CLAIMS:

Please amend the claims as follows.

1. (Amended) A method of operating an authenticating server system for authenticating users at client terminals connected via a data communications network, to control access to a document stored on a resource server, said method comprising performing the following in said server system:

storing authentication details of authorized users;

receiving authentication data for a user from a client terminal of the user and validating said authentication data by reference to said stored authentication details;

issuing an identifier for the user's client terminal to said terminal for storage thereon, the identifier being transmitted in such a manner that the identifier is retransmitted by said user's client terminal with document requests directed at said resource server;

storing status data indicating said identifier to be a validated identifier of a terminal of a currently authenticated user, in response to the receipt and validation of the authentication data; and

enabling said resource server to validate a request for said document from the user's client terminal, which request includes said identifier, by checking said status data on receipt of said document request.

Sub C7

2. (Amended) A method according to claim 1, wherein said identifier is transmitted in a cookie to said user's client terminal.

B9

3. (Twice Amended) A method according to claim 1, wherein said identifier is received from said user's client terminal with said authentication data.

4. (Amended) A method according to claim 3, wherein a new identifier is issued to said user's client terminal if said authentication data is invalid.

5. (Amended) A method according to claim 4, wherein said identifier comprises data indicating the number of times an invalid authenticator has been received from said user's client terminal.

6. (Amended) A method according to claim 5, wherein said method comprises issuing no further identifier to said user's client terminal if an identifier received from said user's client terminal indicates that a

predetermined number of invalid authenticators have been received from said user's client terminal.

7. (Twice Amended) A method according to claim 1, comprising timing out said identifier as an identifier of a terminal of a currently authenticated user if no document request is received from said user's client terminal for a predetermined period.

8. (Twice Amended) A method according to claim 1, comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain; and

enabling each of said Web servers to validate document requests from the user's client terminal, which requests include said identifier, by checking said status data on receipt of a document request.

9. (Amended) A method of operating an authenticating server system for authenticating users at client terminals remotely connected via a data communications network, to control access to a plurality of resource servers, said method comprising performing the following steps in said server system:

storing authentication details of authorized users;

performing remote authentication of a user by reference to said stored authentication details and during said remote authentication step generating

status data, distinguishing said user from other users which are not currently authenticated, and a secret encryption key shared with said user;

storing said status data in storage means accessible to said plurality of resource servers to check an authentication status of said user by using an identifier for the user's client terminal received in a service request; and

storing said shared secret key in a data store accessible by at least one of said resource servers for use during communications with said user.

10. (Amended) A method according to claim 9, wherein said remote authenticating step comprises issuing a challenge to the user's client terminal, receiving a response to said challenge, and verifying said response.

14. (Twice Amended) A method according to claim 12, wherein said updating step is performed in response to a request by the user's client terminal.

15. (Twice Amended) A method according to claim 9, wherein said identifier is an IP address of the user's client terminal.

16. (Twice Amended) A method according to claim 9, wherein said authentication step comprises issuing said identifier to the user's client terminal.